Fault Tree In the Trenches, A Success Story

R. Allen Long: Hernandez Engineering, Inc., Huntsville, Alabama

Keywords: fault tree, cutsets, hardware, analysis

Abstract

Getting caught up in the explanation of Fault Tree Analysis (FTA) minutiae is easy. In fact, most FTA literature tends to address FTA concepts and methodology. Yet there seems to be few articles addressing actual design changes resulting from the successful application of fault tree analysis.

This paper demonstrates how fault tree analysis was used to identify and solve a potentially catastrophic mechanical problem at a rocket motor manufacturer. While developing the fault tree given in this example, the analyst was told by several organizations that the piece of equipment in question had been evaluated by several committees and organizations, and that the analyst was wasting his time. The fault tree/cutset analysis resulted in a joint-redesign of the control system by the tool engineering group and the fault tree analyst -- as well as bragging rights for the analyst. (That the fault tree found problems where other engineering reviews had failed was not lost on the other engineering groups.) Even more interesting was that this was the analyst's first fault tree which further demonstrates how effective fault tree analysis can be in guiding (i.e., forcing) the analyst to take a methodical approach in evaluating complex systems.

Introduction

The first fault tree I performed was one of my most resounding successes. Not only did the tree identify previously undiscovered failure mechanisms, but also resulted in tooling engineering and the safety organization (i.e., Hazards Analysis Department) jointly redesigning the tooling control system. Future relations and cooperation between the Hazards Analysis Department and other engineering groups were also greatly enhanced as a result of us finding substantive enhancements to a design.

Let's Get Started

My first fault tree was for a piece of lifting equipment called the "Vaculift". The Vaculift is considered a breakover fixture, in that it allows operators to lift and rotate a large cylindrical rocket motor case from horizontal to the vertical position and vice versa. Dropping a motor case due to a Vaculift malfunction, error or failure was considered catastrophic. Releasing a cylinder while suspended in the air could easily kill someone. Each motor case is 12 feet in diameter and weighs, well ... a lot. Since the lifting operations took place indoors, sometimes with small clearances, a person could be squashed even though personnel were strictly forbidden to stand under the Vaculift and cylinder. The case was expected to roll if dropped. In addition, the program considered damaging the motor case just short of being monetarily catastrophic.

Supplied with this basic description and a vacuum system schematic I was fed to the wolves.

Trial By Fire

Several engineering groups and committees had evaluated the Vaculift and established there were no single-point failures in the hydraulic or vacuum systems of the Vaculift. Various engineering groups openly let me know my management was having me perform the safety equivalent to being sent to find a left-handed monkey wrench. Within about a week however, I found the redundant vacuum systems were tied into a single venting switch and relay. As soon as this was discussed with several engineers and managers, I was encouraged to widen my fault tree to include the whole system. The engineers who originally smirked at my task were now quite cooperative. In fact, the Hazards Analysis Department earned a grudging respect from several engineering groups at the facility. Much of the success of this analysis can be attributed to information gained through talking with and watching the equipment operators. Drawings do not always tell you what is going on in the actual implementation and operation of a design – only how the design is supposed to operate. Several interesting problems were discovered through

observations on the shop floor – problems which could have easily been overlooked if the analysis had been based strictly on the Vaculift drawings. At this point a friend and colleague of mine, W. Cliff Whitlock joined me on the project. Cliff was initially brought in to help me identify all the possible switch failure / activation combinations which could contribute to the different scenarios. Cliff also single-handedly developed a computer program to calculate the cutsets from the tree. Remember this was 15 years ago -- prior to fault tree programs such as Integrated Reliability and Risk Analysis System (IRRAS). Equally amazing, was L. Dave McLean's validation of the computer program. Dave, who was my supervisor at the time, calculated all 750 cutsets (437 minimal cutsets) by hand! It was also at this time, we began closely working with the tool engineer responsible for the control system. By the time our report was issued, Redesign Ladder Diagrams of the electrical control system were already complete and included in the report.

Inside the Grand Gizmo

Figures 1 and 2 show what the outside of the Vaculift looks like. The Vaculift consists of two arms each mounted to rotating array of vacuum pads. Each array consisted of seven vacuum pads mounted on a load beam. (The vacuum pad arrays are referred to as the vacuum legs). Together the two arrays or "legs" clamp down and provide the

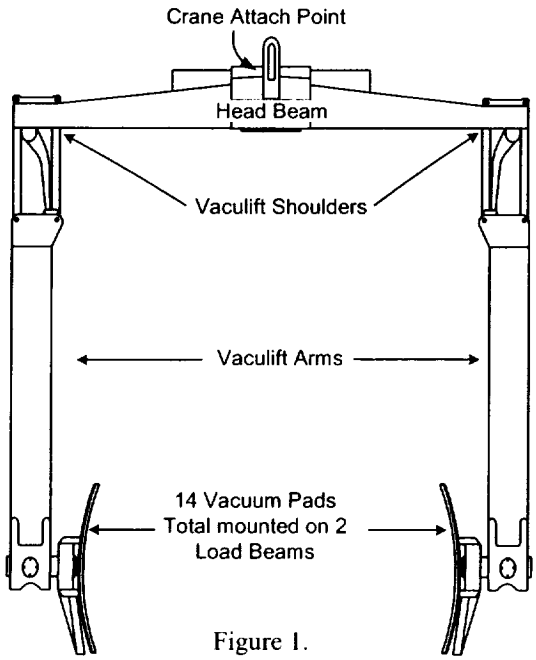

Figure 1.

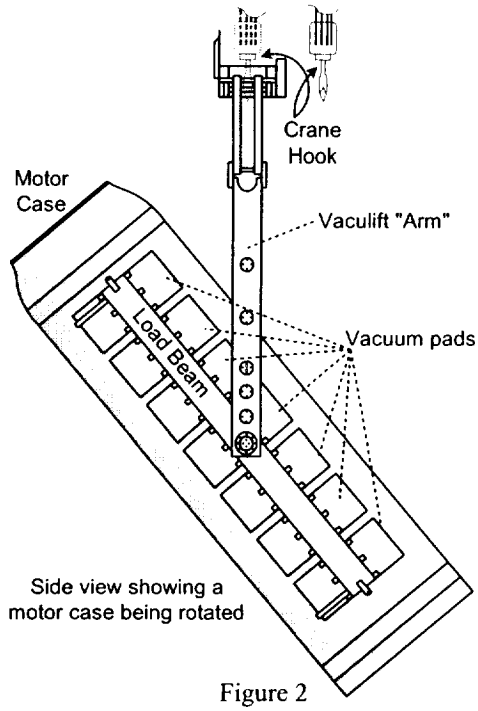

Figure 2

motor case holding force when vacuum is pulled on all 14 pads. Vacuum is pulled by two independent vacuum systems. Two independent hydraulic systems (one for each leg / arm pair) allow the "arms" to move in or out at the shoulders of the main lifting support beam (i.e., the Head Beam). These hydraulic systems also provide power for rotating the case via the vacuum leg. Each vacuum leg can be rotated independently for proper positioning of the Vaculift onto the motor case until vacuum is pulled. Once vacuum was pulled, the legs were only to be rotated in unison per a procedure. A crane hook capture feature was incorporated into the Vaculift to allow an overhead crane to lift the Vaculift and case without possibility of the crane hook dislodging from the crane attach point.

Inside the Vaculift was truly a beautiful piece of engineering. There were two completely redundant vacuum systems. Virtually anything on one system could fail without affecting the other vacuum system. A motor case could be raised and rotated with a single working vacuum system. Vacuum pads from each vacuum system were alternated on the Vacuum Pad Array, such that one system provided vacuum to four pads on one array and 3 pads on the other array. I must add, though, that lifting with only a single functioning vacuum system was never allowed. The

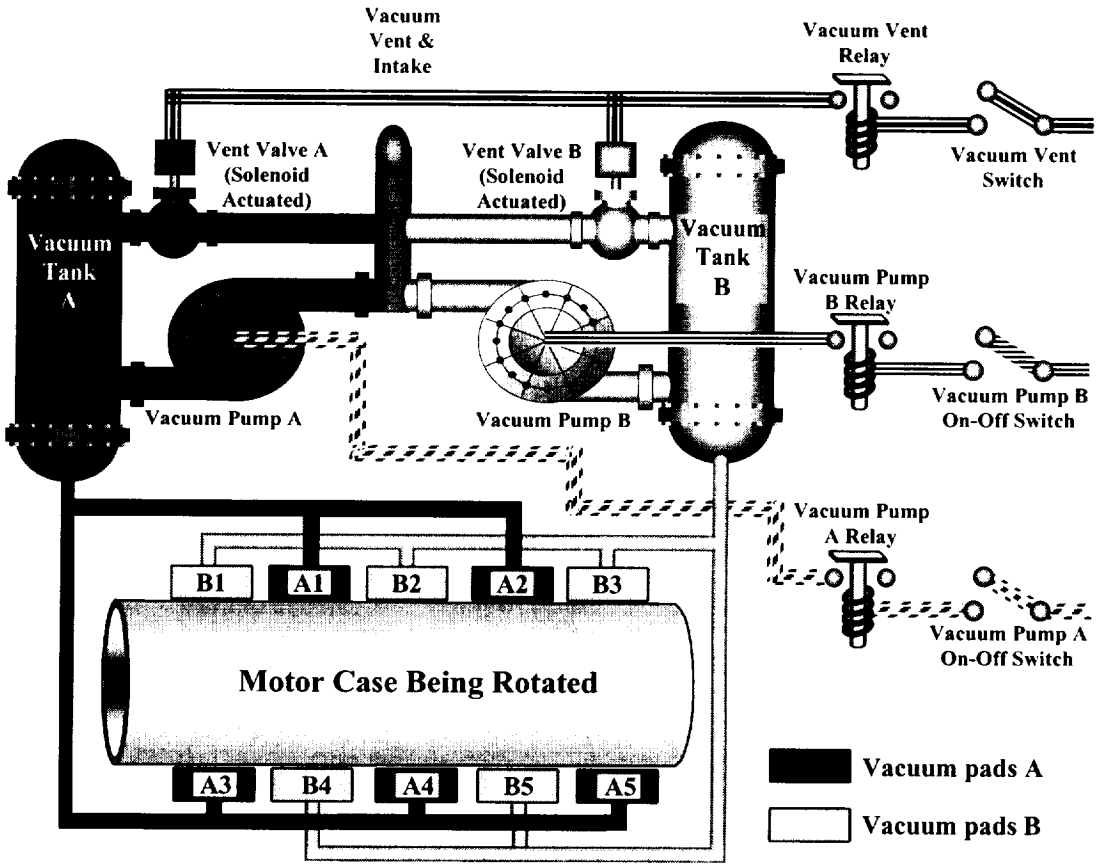

Figure 3

redundant vacuum systems were in place to prevent dropping the motor case if vacuum were to be lost in one of the systems during a lift. A low vacuum alarm was in place to let operators know if loss of vacuum occurs during a lift.

Figure 3. shows a simplified version of the vacuum systems configuration.

Interfacing Up to the Problem. Interfaces are one of the most talked about items in our industry, but too often little is done to adequately analyze and/or deal with them. In the case of the Vaculift this was especially true. Two separate engineering departments were in charge of designing the Vaculift. The tooling engineer designing the mechanical portion of the Vaculift including the vacuum system did an absolutely superb job on the redundant vacuum system. However, the engineer in charge of the control system connected the venting systems of both vacuum systems to a single switch and relay. Failure or activation of the switch or relay would vent the vacuum to both systems at the same time and release the cylinder.

Redundant Does Not Always Equal Safe. In the case of the hydraulic system used to rotate the cylinder, complete redundancy was actually a potential cause of a catastrophic failure. Both hydraulic systems were totally independent of each other. In addition, each of the two hydraulic systems rotated its own vacuum leg. If one hydraulic pump stopped, the leg it was controlling would stop rotating. However, the other hydraulic pump would continue to rotate its leg until it popped the motor case from between the two arrays. Compounding the likelihood of twisting a case from between the arrays during a hydraulic pump failure was a lack of an emergency stop for the hydraulic system on the controls. The hydraulic power was tied into the vacuum system power forcing operators to shut off the vacuum system to stop the hydraulic system.

Back to the Fault Tree

Now that I have basically given away the two most major problems discovered during the fault tree analysis, let's discuss a little more in depth

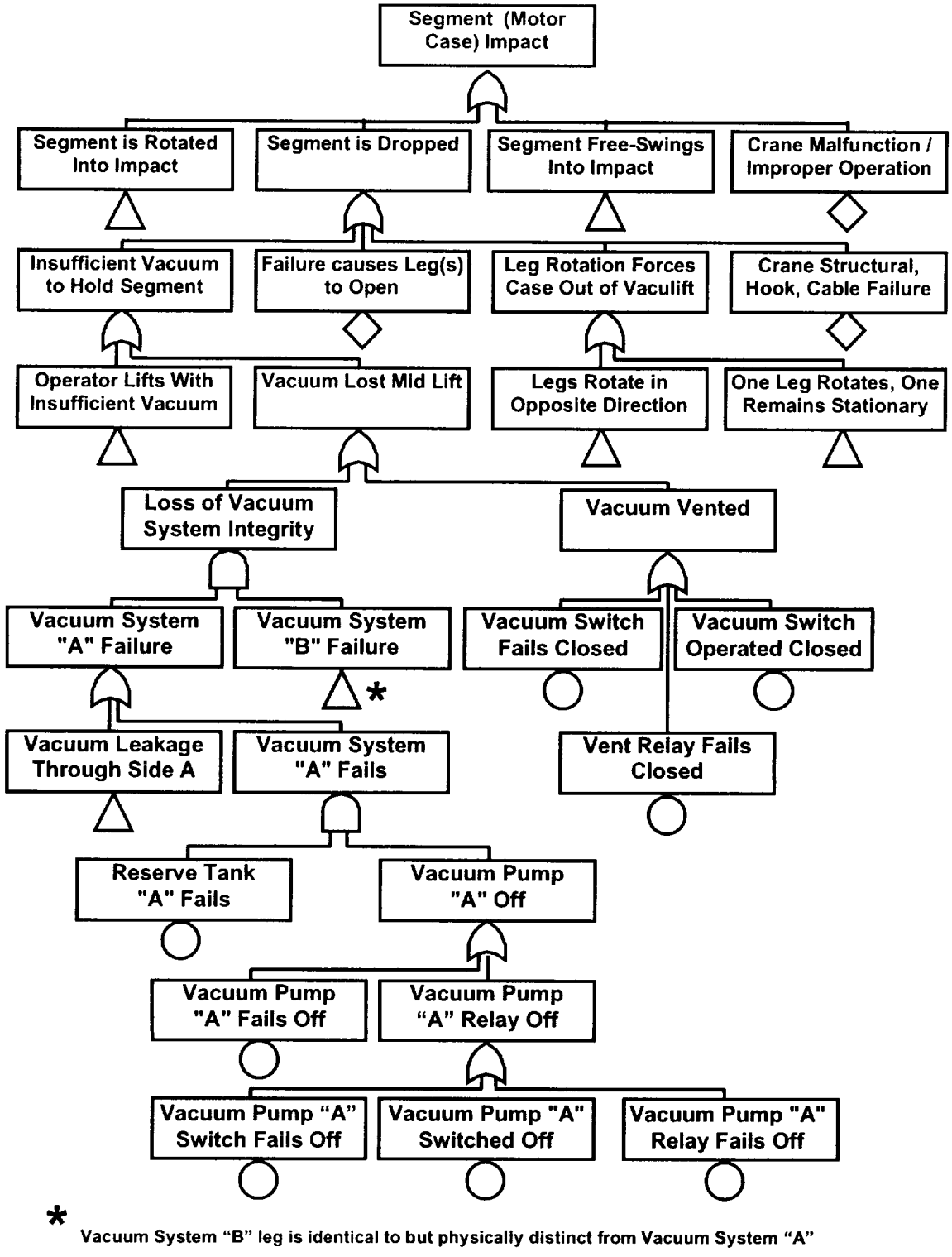

Figure 4

the process used to ferret out the problems. There were several other issues that were also uncovered by the analysis which I will address later.

Figure 4 shows a portion of the fault tree. The tree has been simplified in several undeveloped areas in order to fit into this paper. (e.g., the block "Crane Structural, Hook, Cable Failure" was originally several blocks which included failure

failure of the Vaculift hook attach point.) There have also been several updates to the tree to implement lessons I have learned over the years about fault tree organization.

The basic premise was to find anything in the design and operation of the Vaculift which could cause an impact to the motor case. Vaculift operations provided several of its own means of causing impact. In addition, the Vaculift was hoisted and moved with a crane, which provided additional potential ways of causing case impact. The short version is that we could:

- Drop the case due to a crane structural failure
- Drop the case by releasing vacuum pressure
- Drop the case by opening the Vaculift arms
- Impact the case by rotating the case into the ground or object. This could be due to either actively rotating the case, or due to free-swinging due to structural failure of the rotational drive train.
- Impact the case by moving the case into an object via the crane
- Drop the case by popping the case from between the vacuum legs by rotating the legs opposite of each other (or by having a single leg stop and the other continue to rotate)
- Drop the case due to Vaculift structural failure.

Virtually any of these events could be caused by a hardware malfunction or by a operator functional error (e.g., activation of a switch at the wrong time). In automated systems which use a programmable controller or computer, these functional errors are handled basically the same. Rather than an operator accidentally activating the switch, a fault tree for an automated system should include command error due to feed-back (i.e., sensor) error, controller failure, or software error for each and every switch, valve, or other actuation possibility.

Where do we start? The first step was to ground-rule out crane functional and structural failure for purposes of the fault tree. The emphasis of this exercise was to concentrate on the Vaculift contribution to case damage due to impact. Crane Failure is listed on the fault tree as an undeveloped event to show that we recognize crane failure as a valid means of causing case impact during Vaculift operations. However, for purposes of the fault tree crane failure has been deemed out-of-scope. This is not to say that crane operation was completely swept aside and forgotten. Watching the Vaculift-ing operations, talking to operators and crawling over the equipment, including the crane controls, revealed that there was no emergency stop on the crane pendant control. Even though this was not within the scope of the fault tree per se, failure to recommend an emergency stop for the crane would have been a serious omission in the fault tree report.

The next step was to look at the structural strength of the Vaculift. Traditionally, ground based systems can have high structural safety margins since weight is usually of little relative concern. The Vaculift was no exception. In fact, margins on the Vaculift were so high that if your car had the same structural strength, you could use it as a mobile bomb shelter. The margins were recorded in the fault tree report and "Structural Failure" placed in the fault tree as undeveloped .

We also discovered relatively quickly, that opening the arms of the Vaculift under pressure and dropping the case was unlikely since the hydraulic rams for spreading the arms were under-powered by design. They simply did not have the horsepower to spread the arms even if inadvertently activated. Theoretically, we probably should have developed the scenario further since spreading the arms with insufficient vacuum would have dropped the case. However, this would probably have been minimized out in the cutsets anyway (How is that for a good save?).

"Start With Functional And / Or Operational Scenarios -- Not With Subsystem Failures"

A common mistake by those new to fault tree analysis is to immediately break the system down into subsystem failures rather than the functional scenarios which could cause the top undesired event. This is also common when the engineer developing the tree is not a systems person. You will notice that the Vaculift fault tree was arranged at the top levels by all the possible scenarios which could cause impact. "Failures" such as electrical and mechanical failures were addressed, but not at the higher levels. Since this

was my first fault tree, I am not sure this was due to sheer luck or that I was thinking logically!

The reason this concept is so important is that the Top Undesired Event is often caused by a functional anomaly of several subsystems. And, there are usually different ways in which these combinations manifest themselves. Even more important is that a poor design can cause or contribute to the Top Undesired Event without a failure (i.e., normal functioning of a system under specific operating conditions can cause the Top Undesired Event).

Let's look at an instance for which "Electrical Failure" at the top of the tree could have prevented us from discovering a particular problem with the alarm system. Such was the case with the "Low Vacuum Alarm". The vacuum alarm was a major contributor to the Top Undesired Event WITHOUT A FAILURE! A latching relay was in place to prevent the alarm from wailing while the initial vacuum was being pulled on the case. When proper vacuum was attained, the latch relay would engage the alarm. However, if operators lifted the case prior to getting proper vacuum (i.e., sufficient vacuum to lift the case but insufficient vacuum to engage the latch relay) the alarm would not sound if a leak were to occur. The operators could also lift the case with insufficient vacuum in the first place, thereby immediately dropping the case. Even though there was a light to indicate whether vacuum was properly attained the light had burned out and no one had noticed. Furthermore, none of the indicator lights incorporated "Push-To-Test" switches. Therefore it was not possible for the operators to know whether the light was working. This is not to say electrical failure of the alarm could not contribute to the Top Event. Failure of the latch relay to engage would silence the alarm even after proper vacuum were attained. A vacuum loss in the system would remain undetected.

The solution to this problem included eliminating the latch relay and installing a two-way key-switch. The key-switch would disable the alarm while pulling the vacuum initially. However, it also disabled the lifting function of the crane as well. When the switch was turned to the "Test/Lift" position, the alarm and lifting functions were enabled. Hence, operators could not unknowingly lift without proper vacuum since the alarm would sound as soon as the switch was turned to the Test/Lift position. In addition, all indicator lights were replaced with push-to-test switches and labeled as such on the control pendant. An alarm test button was also installed on the control pendant.

All recommendations were "Theoretically failed" to ensure we were not increasing potential hazards to the system with our solutions. In the case of the two-way key-switch on the alarm failing in the "Alarm Off" Position would also disable the lifting function of the crane (but not the "Lower" function. Removing the latch relay only increased the reliability of the alarm system. We were no worse off than prior to the redesign if the "Push-To-Test" indicator lights / buttons were to fail.

An Exception and Caution to the "Start With Scenarios" Rule

"Structural Failure" is often an exception to the rule, "*Start with functional and/or operational scenarios and not with subsystem failures.*" Care must be taken to ensure that *induced* structural failures are developed as well as the simple structural failures. For instance a load may be well under the rated capacity of the crane lifting the load. However, if the load has been strapped down to a truck and was not un-strapped prior to lifting, the crane can come tumbling down.

Vaculift Findings and Recommendations

Now let's recap some of the groundrules for the Vaculift Fault Tree Effort:

1. The fault tree examined more than just failures and included:
   - Operational and functional scenarios
   - Non-failure-related design problems
   - The as-built configuration and current condition of hardware
   - Operators' use of the system
2. All Recommendations were evaluated and "Failed" as applicable to ensure additional or worse hazards were not introduced.
3. Recommendations were based on improving the hardware and system and not requiring additional precautions and procedures for operators to have to follow.

What were some of the findings and solutions we came up with?

1. In my first example, a single switch activation or failure, or a single relay failure, would cause immediate venting of the vacuum and the motor case to be dropped.

   We solved this problem by:

   - Eliminating the relay. The relay was specifically in the circuit to allow a single switch to vent both systems by design!
   - Installing separate vacuum vent switches for each of the two systems. Both vent switches were keyed with the same key. Only one key was allowed on the floor. Operators could not throw both vent switches at the same time.

2. My second example included several problems with the hydraulic system used to position and rotate the vacuum legs In this example, there were three hydraulic rotate switches: A "Leg A" Rotate Switch, a "Leg B" Rotate switch and a "Legs" Rotate switch (For rotating both legs at the same time):

   - Hydraulic Systems were completely redundant. Failure of a single pump would stop one side. The other side would continue to rotate.
   - Hydraulic power and Vacuum pump power were tied together. The hydraulic system could not be stopped in an emergency without shutting off the vacuum.
   - There was no Emergency Stop for the hydraulic system.

   The solutions included:

   - Installing an emergency stop for the hydraulic system.
   - Re-wiring hydraulic and vacuum power so that they receive power independently of each other.
   - Interlocking the independent rotation switches through a relay which cut power from "Leg A" and "Leg B" Rotate switches once the vacuum system was activated.
   - Plumbing the two hydraulic pumps in parallel or eliminating one of the pumps. Failure of a single pump would not allow the other pump to rotate a single leg. Plumbing both pumps through a common manifold would allow the Vaculift to "fail-safe" AND "fail-operate" during a single pump failure. Eliminating one of the pumps and running both hydraulic systems with a single pump would have a "fail-safe in Off" condition.

The End Results

So, what became of our recommendations? First, there was a committee formed basically to disprove our conclusions and recommendations. However, with the exception of some proximity sensor recommendations, all our recommendations were accepted and implemented. This included adding an emergency stop button to the crane controls. We had recommended proximity sensors to stop operators from accidentally rotating the case into the ground. Based on the maturity, complexity and reliability of proximity sensor systems at the time, the operating organization was justifiably concerned that operations would be constantly shut-down erroneously.

After several months the recommendations were incorporated. There was no redesign period since we had worked all recommendations with the responsible tool engineer. The reason our recommendations passed muster of the "Disapproval Committee" was mostly due to our close work along the way with the tool engineer. The tool engineer helped to ensure we thoroughly understood the system and that none of our recommendations were stupid or non-functional. Now came the day for testing the improved Vaculift.

Operators fired up the Vaculift and it promptly refused to operate! The tool engineer scrambled through the drawing he had brought to the test. As we looked through the drawing, the first thing on our minds was that we *had* done something stupid or non-functional with the design. Thankfully, the design was correct. Evidently "Joe Maintenance" had wired several solenoids backwards from our design. "As-Designed" vs. "As-Built" in the same sentence is often an oxymoron. A single maintenance person, technician, mechanic, or electrician can undo the work of an entire design team in an instant.

But ... that is a subject for another paper!

Biography

Allen Long, Senior System Safety Engineer, Hernandez Engineering, Inc., MSFC, AL 35812 USA, Telephone – (256) 961-1177, facsimile – (256) 544-8022, e-mail – allen.long@msfc.nasa.gov

Allen Long is a Senior System Safety Engineer for Hernandez Engineering, Inc. on the Safety and Mission Assurance Contract at Marshall Space Flight Center (MSFC). He specializes in hazards analysis FTA for systems and process design. Mr. Long is considered the MSFC resource person for FTA and regularly performs FTA for Development Programs as well as for existing systems and mishap investigations. Mr. Long was awarded both Engineer of the Year and Best Paper Awards at the 17th International System Safety Conference. Past fault trees have included X-34 Hydraulic System, X-33 Linear Aerospike Engine and Ground Support Systems design, Chandra X-Ray Telescope, Gravity Probe B, and Transfer Orbit Stage. He has been responsible for FTA on the majority of mishap investigations at MSFC for the 12 ten years on programs including both Tethered Satellite System (TSS) missions. Prior to working at MSFC Allen worked for the Hazards Analysis Department at Thiokol in Brigham City Utah, and at Hercules, Inc., in Magna, Utah as a line safety engineer.